Министерство образования Республики Беларусь
Учреждение образования
«Полоцкий государственный университет»

ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ: ДОСТИЖЕНИЯ, ПРОБЛЕМЫ, ИННОВАЦИИ (ИКТ-2018)

Электронный сборник статей
I Международной научно-практической конференции,
посвященной 50-летию Полоцкого государственного университета

(Новополоцк, 14–15 июня 2018 г.)

Новополоцк
Полоцкий государственный университет
2018

Информационно-коммуникационные технологии: достижения, проблемы, инновации (ИКТ-2018) [Электронный ресурс] : электронный сборник статей I международной научно-практической конференции, посвященной 50-летию Полоцкого государственного университета, Новополоцк, 14–15 июня 2018 г. / Полоцкий государственный университет. – Новополоцк, 2018. – 1 электрон. опт. диск (CD-ROM).

Представлены результаты новейших научных исследований, в области информационно-коммуникационных и интернет-технологий, а именно: методы и технологии математического и имитационного моделирования систем; автоматизация и управление производственными процессами; программная инженерия; тестирование и верификация программ; обработка сигналов, изображений и видео; защита информации и технологии информационной безопасности; электронный маркетинг; проблемы и инновационные технологии подготовки специалистов в данной области.

Сборник включен в Государственный регистр информационного ресурса. Регистрационное свидетельство № 3201815009 от 28.03.2018.

Компьютерный дизайн М. Э. Дистанова.

Технические редакторы: Т. А. Дарьянова, О. П. Михайлова.

Компьютерная верстка Д. М. Севастьяновой.

211440, ул. Блохина, 29, г. Новополоцк, Беларусь
тел. 8 (0214) 53-21-23, e-mail: irina.psu@gmail.com

ISBN 978-985-531-602-3

УДК 004.738.5:339

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В ЦИФРОВОЙ ЭКОНОМИКЕ

магистр техн. наук В.С. КНЯЗЬКОВА
(Белорусский государственный университет информатики и радиоэлектроники, Минск)

Многочисленные изменения, вызванные современной цифровой средой и получившие широкое распространение посредством информационно-коммуникационной инфраструктуры, значительно расширили масштабы проблем информационной безопасности и конфиденциальности. Все это привело к необходимости эволюции представлений об эффективном управлении цифровой безопасностью и рисками конфиденциальности как на уровне стран и мирового сообщества, так и на уровне организаций. Повышение доверия к цифровым услугам со стороны пользователей и клиентов позволит расширить возможности их использования. Именно доверие играет важную роль в ситуациях, где существует неопределённость и взаимозависимость, и цифровая среда, представляющая собой распределенную систему, несомненно, является именно таковой.

Современная цифровая экономика опирается на сложную систему, состоящую из множества тесно связанных между собой элементов, которая технологически основывается на информационно-коммуникационных технологиях (ИКТ) и обработке больших потоков данных («Big Data»), а также на мобильных соединениях и использования сети Интернет в том числе для подключения к ней огромного числа компьютеров и устройств с специальными радиочастотными метками («Интернет вещей») [1]. Расширяющиеся возможности подключения все большего числа устройств и обработки полученных данных добавляют системе сложность, волатильность и зависимость от инфраструктур и процессов, которые не полностью находятся в рамках единого юрисдикционного и организационного контроля [2, 3]. Таким образом, угрозы информационной безопасности представляют собой проблему межотраслевого взаимодействия, в которую вовлечены множественные стейкхолдеры. То, что происходит в малом (или, к примеру, частном бизнесе), может повлиять на крупный бизнес (или государственные организации) и на всех других участников цепочки создания стоимости. Организации, независимо от того, функционируют ли они в государственном или частном секторе, несомненно, выигрывают от такой тесной взаимозависимости благодаря распространению инноваций и лучших управленческих практик, что в конечном итоге приводит к повышению эффективности работы организаций [4, 5, 6]. Такой интенсивный обмен и использование больших потоков данных также могут способствовать нарушению конфиденциальности персональных данных и созданию цифровых угроз безопасности. Необходимо признать повышение неопределенности, которая возникает в результате этих новых событий и одновременно необходимость эволюции существующих стратегий минимизации цифровых угроз безопасности и конфиденциальности.

В настоящее время существуют различные технологические решения для повышения информационной безопасности. Тем не менее, для того, чтобы оптимизировать

экономические и социальные выгоды от открытой цифровой среды, необходимо перейти от рассмотрения рисков информационной безопасности исключительно как технического вопроса к использованию тех методик, которые в настоящее время используются в управлении экономическими и социальными рисками. Отметим, что такое решение предлагается в Рекомендациях ОЭСР по управлению рисками в области цифровой безопасности для экономического и социального процветания [7] (далее – Рекомендации ОЭСР по УРЦБ). Данный документ содержит рекомендации руководителям и/или лицам, ответственных за принятие решений, интегрировать управление рисками информационной безопасности в процессы принятия экономических и социальных решений.

Аналогичные рекомендации содержатся и в еще одном документе ОЭСР – Руководстве по конфиденциальности. В нем подчеркивает важность применения концепции риска в цифровой экономике, а также предлагается Программа управления конфиденциальностью, которая формулирует основные принципы конфиденциальности и условия их достижения. Защита данных и личной информации также должны быть частью общей стратегии управления рисками организации. Эти аспекты могут создавать дополнительные конкурентные преимущества и предоставлять инструменты для более эффективного использования инноваций и повышения производительности. И партнеры, и клиенты предпочитают работать с теми организациями, которые обеспечивают конфиденциальность информации.

В Рекомендациях ОЭСР по УРЦБ под риском цифровой безопасности понимают тот риск, который связан с использованием, развитием и управлением цифровой средой в процессе любой деятельности. Этот риск может быть результатом сочетания угроз и уязвимостей в цифровом окружении и привести к уменьшению эффективности социально-экономической деятельности. Риски цифровой безопасности по своей природе являются динамическими, что обусловлено физическими законами и спецификой цифрового окружения, а также участием в данных процессах человека [8]. Под процессом управления рисками цифровой безопасности в Рекомендациях ОЭСР по УРЦБ понимают последовательность согласованных действий внутри или между организациями с целью максимального использования возможностей для минимизации угроз цифровой безопасности; при этом следует соотносить эффект от использования определенных мер по обеспечению цифровой безопасности с затратами на их реализацию.

Отметим, что так как цифровая среда предполагает еще большую взаимозависимость между ее участниками, чем традиционная, игнорирование вопросов обеспечения ИБ одним экономическим агентом может увеличивать риски ИБ для других. Следовательно, повышение осведомленности, знаний и навыков в сфере ИБ целевой аудитории облагает синергетическим эффектом, распространяющимся по всей социально-экономической системе ЭБ, выражающимся главным образом в снижении общего уровня риска ИБ ЦБ.

Таким образом, повышение знаний в сфере ИБ ЭБ должно быть направлено в том числе и на область возможных технических и социально-экономических последствий реализации угроз ИБ. Также необходимо мотивировать участников цифровой среды постоянно повышать свой уровень знаний и компетенций в этой области, принимать во внимание динамический характер рисков ИБ и факторов, влияющих на них. Все это требует создание непрерывного процесса, интегрированного в процессы управления рисками.

Литература

1. Data-Driven Innovation: Big Data for Growth and Well-Being [Electronic resource] : OECD Publishing, Paris, 2015. – Mode of access: http://dx.doi.org/10.1787/9789264229358-en. – Date of access: 01.03.2018.
2. Managing digital security and privacy risk. Background report for Ministerial Panel 3.2 [Electronic resource] : OECD Directorate for science, technology and innovation, Committee on digital economy policy, 01.06.2016. – Mode of access: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG (2016)1/FINAL&docLanguage=En. – Date of access: 01.03.2018.
3. OECD Digital Economy Outlook 2017 [Electronic resource] : OECD Publishing, Paris, 2017. – Mode of access: http://dx.doi.org/10.1787/9789264276284-en. – Date of access: 01.03.2018.
4. Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy [Electronic resource] : OECD Digital Economy Papers, № 211, 2012. – Mode of access: http://dx.doi.org/10.1787/5k8zq92vdgtl-en. – Date of access: 02.03.2018.
5. Oslo Manual: Guidelines for Collecting and Interpreting Innovation Data, 3rd Edition [Electronic resource] : OECD and Eurostat, 2005. – Mode of access: http://dx.doi.org/10.1787/9789264013100-en. – Date of access: 02.03.2018.
6. Создание глобальной культуры кибербезопасности [Электронный ресурс] : одобр. резолюцией 57/239 Генер. Ассамблеи, 31 янв. 2003 г. // Организация Объединенных Наций. – Режим доступа: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/57/239&referer=/english/&Lang=R. – Дата доступа: 02.03.2018.
7. Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document [Electronic resource] : OECD Publishing, Paris, 2015. – Mode of access: http://dx.doi.org/10.1787/9789264245471-en. – Date of access: 01.03.2018.
8. Guide for conducting risk assessment. Special publication 800-30, revision 1 [Electronic resource] : NIST, 2012. – Mode of access: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf. – Date of access: 02.03.2018.